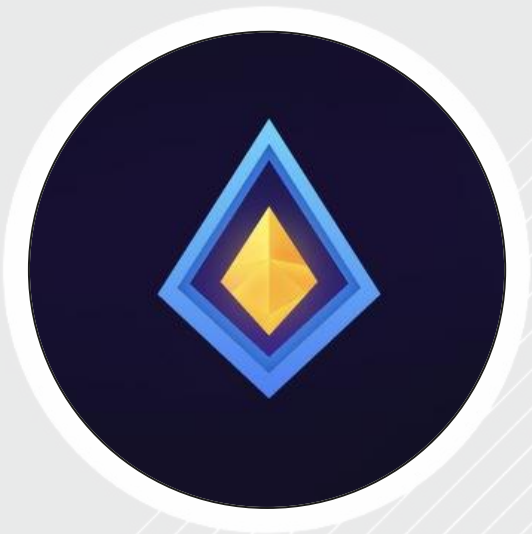
SPYWOLF

Security Audit Report



Completed on

November 16, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **STELLUM** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

Clarification

The following audit includes **only** the game mechanics contract.
There are 3 contracts involved in the game:

- Game mechanics contract
- SGT Token contract
- NFT contract

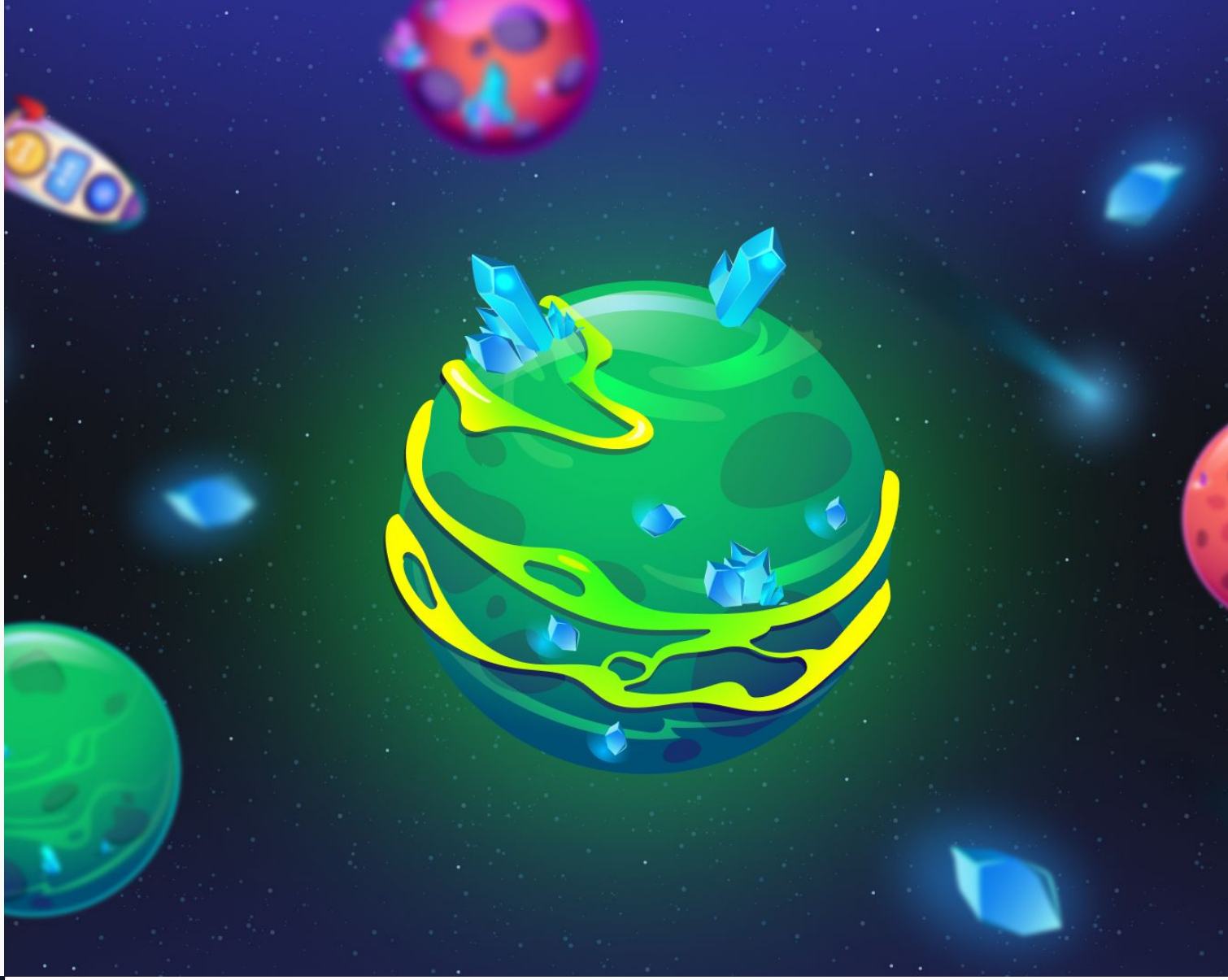
The NFT contract and SGT Token contract are **out of the scope** of this audit and we are unaware of the content of these contracts - and it can be potentially harmful

The three contracts are closely linked and relies in each other in order for the game to function as intended.

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

TABLE OF CONTENTS

STELLUM



PROJECT DESCRIPTION

According to their whitepaper:

Stellum is a play to earn game with NFT characters that open up opportunities not only for an interesting game, but also to receive cryptocurrency.
Explore space, discover new planets, hire workers to extract resources and most importantly - improve your NFT character.
The NFT character is your key to lucrative SGT earning events and entry to the project's next P2E products.

Release Date: Presale starts in November, 2022

Category: P2E/NFT

CONTRACT INFO

Token Name
Sellum

Symbol
N/A

Contract Address
0x71f335aD4a6635B53610285a3Ec265E6Ca794967

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Nov 16, 2022

Verified?
Yes

Total Supply
N/A

Status
Not launched

TAXES

Buy Tax
10%

Sell Tax
n/a

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of November 16, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount	Additional Info:

LP Address(es)

Liquidity not added yet

Planet levels: 50

NFT Price: 0.1 BNB

NFT Max Supply: 10,000

Character levels: 20

TOKEN TRANSFERS STATS

Transfer Count	N/A
Uniq Senders	N/A
Uniq Receivers	N/A
Total Amount	N/A
Median Transfer Amount	N/A
Average Transfer Amount	N/A
First transfer date	N/A
Last transfer date	N/A
Days token transferred	N/A

SMART CONTRACT STATS

Calls Count	6
External calls	6
Internal calls	0
Transactions count	6
Uniq Callers	3
Days contract called	1
Last transaction time	2022-11-16 15:02:02 UTC
Created	2022-11-16 14:29:22 UTC
Create TX	0xe00ce508f8a76c323531276fa1ab27e0f5d91cc78cdfcf84c62adc8669b90fe0
Creator	0xcc756b666781b9f8104676c0d1cd06c76079288b

FEATURED WALLETS

Owner address	0xcc756b666781b9f8104676c0d1cd06c76079288b
Promotion address	0x0f2e395e26296d0ec3769f829186a05c621fe144
LP address	0x5FE09F811273E1c5A23b3DB80B1f14BbB3125fd6

TOP 3 UNLOCKED WALLETS

1 N/A

2 N/A

3 N/A

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can change buy back percent up to 100%.
When user makes a purchase, percent of this purchase goes towards buyback of SGT tokens which are paired in liquidity pool.
Tokens bought goes to wallet controlled by owner (PROMOTION_ADDRESS).

```
function changeTokensBuyBackPercent(uint8 percent) external onlyOwner {
    require(percent > 0 && percent <= 100, "Invalid percent value");

    TOKENS_BUY_BACK_PERCENT = percent;
}

function buyEnergy(address referrer) external payable {
.......................
buyBackTokens(address(this).balance * uint256(TOKENS_BUY_BACK_PERCENT) / 100);
addLiquidity(address(this).balance);
.......................
}


function buyBackTokens(uint256 bnbAmount) private {
address[] memory path = new address[](2);
path[0] = address(0xbb4CdB9CBd36B01bD1cBaEBF2De08d9173bc095c); // Wrapped BNB (WBNB)
path[1] = ERC20_TOKEN_ADDRESS;

IPancakeRouter(PANCAKE_ROUTER_ADDRESS).swapExactETHForTokens {value: bnbAmount} (
  0,
  path,
  PROMOTION_ADDRESS,
  block.timestamp + 5 minutes
);

//TODO: emit event
}
```

- Recommendation:
  - Consider reasonable upper limiter for the buy back percent variable.

FOUND THREATS

⚠ High Risk

Owner of STM token contract can add minters.
Minters can mint (create) new tokens.
This can lead to liquidity drain.

```
function addMinter(address minterAddress) external onlyOwner {
    require(Address.isContract(minterAddress), "Only contract may be a minter");

minters[minterAddress] = true;
}

function mint(address to, uint256 amount) external onlyMinter {
    _mint(to, amount);
}
```

FOUND THREATS

⚠ High Risk

Owner of STM token contract can mint new team tokens 180 days after the contract deployment and once each 30 days further on.

```
uint256 public constant TEAM_MINT_PERCENT = 10;
uint256 public constant TEAM_MINT_PERIOD = 30 days;
uint256 public constant TEAM_MINT_1ST_PERIOD = 180 days;

function teamMint() external onlyOwner {
    if (firstTeamMint) {
      require(block.timestamp >= (lastTeamMintTime + TEAM_MINT_1ST_PERIOD), "It's too early");

      firstTeamMint = false;
    } else {
      require(block.timestamp >= (lastTeamMintTime + TEAM_MINT_PERIOD), "It's too early");
    }

    if (totalSupply() <= (lastTeamMintSupply + lastTeamMintAmount)) {
      lastTeamMintTime = block.timestamp;

      return;
    }

    uint256 amount = (totalSupply() - lastTeamMintSupply - lastTeamMintAmount) * TEAM_MINT_PERCENT / 100;

    lastTeamMintTime = block.timestamp;
    lastTeamMintSupply = totalSupply();
    lastTeamMintAmount = amount;

    _mint(owner(), amount);
}
```

FOUND THREATS

⚠ High Risk

Owner of the StellumNFT contract can set new game contact address.
Game contract address can add levels to characters.

```
function upgrade(address playerAddr, uint256 tokenId, uint8 toLevel) external onlyGameContract {
    level[tokenId] = toLevel;

    emit Events.UpgradeCharacter(playerAddr, tokenId, level[tokenId]);
}

function setGameContractAddress(address gameContractAddress) external onlyOwner {
    require(Address.isContract(gameContractAddress), "Invalid Game contract address");
    require(GAME_CONTRACT_ADDRESS == address(0x0), "Game contract address already configured");

    GAME_CONTRACT_ADDRESS = gameContractAddress;
}

modifier onlyGameContract {
    require(msg.sender == GAME_CONTRACT_ADDRESS, "Only Game contract could call this method");
    _;
}

function upgrade(address playerAddr, uint256 tokenId, uint8 toLevel) external onlyGameContract {
    level[tokenId] = toLevel;

    emit Events.UpgradeCharacter(playerAddr, tokenId, level[tokenId]);
}
```

Informational

When users use the buyEnergy() function, new tokens are minted into the STM token contract and paired with bnb in liquidity pair, which is transferred to current contract address.

```
function buyEnergy(address referrer) external payable {
.......................
buyBackTokens(address(this).balance * uint256(TOKENS_BUY_BACK_PERCENT) / 100);
addLiquidity(address(this).balance);
.......................
}


function addLiquidity(uint256 bnbAmount) private {
    uint256 amount = getTokensAmount(bnbAmount);

    ICommonInterface(ERC20_TOKEN_ADDRESS).mint(address(this), amount);
    ICommonInterface(ERC20_TOKEN_ADDRESS).increaseAllowance(PANCAKE_ROUTER_ADDRESS, amount);

    //TODO: emit AddLiquidity(bnbAmount, amount, block.timestamp + 5 minutes);

    (uint256 amountToken, uint256 amountBNB, uint256 liquidity) =
    IPancakeRouter(PANCAKE_ROUTER_ADDRESS).addLiquidityETH {value: bnbAmount} (
      ERC20_TOKEN_ADDRESS,
      amount,
      0,
      0,
      address(this),
      block.timestamp + 5 minutes
    );

    //TODO: emit LiquidityAdded(amountBNB, amountToken, liquidity);

    //TODO: burn LP tokens
}
```

Informational

Owner can manually add liquidity which mints new STM tokens.

```
function addLiquidityManually(uint256 bnbAmount) external onlyOwner {
    addLiquidity(bnbAmount);
}

function addLiquidity(uint256 bnbAmount) private {
.........................
    ICommonInterface(ERC20_TOKEN_ADDRESS).mint(address(this), amount);
    ICommonInterface(ERC20_TOKEN_ADDRESS).increaseAllowance(PANCAKE_ROUTER_ADDRESS, amount);
.........................
}
```

Anyone can withdraw bnb from the contract.
Contract's received bnb is always sent to the promotional address.

```
function buyEnergy() external payable {
    payable(msg.sender).transfer(msg.value);
}

    receive() external payable {
    if (msg.value > 0) {
        payable(PROMOTION_ADDRESS).transfer(msg.value);
    }
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

STELLUM

GOOD PRACTICES FOUND

This is ROI contract paired with STM token. When user make crystals withdraw, SGT token contract issues new tokens accordingly and send them to the user.

Make sure to familiarize yourself with the full game rules content from project’s website and/or whitepaper before investing.

TOKENOMICS

THE TEAM

The team has privately doxxed to SPYWOLF by completing the following KYC requirements:

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

Members KYC'd

KYC Date

May 25, 2022

Format

NFT

Certificate Link

https://opensea.io/assets/matic/0x2953399124f0cbb46d2cbacd8a89cf0599974963/99844844277068474025626073867816441448450620712689519536016720673743692627969.png

THE TEAM

[redacted]

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

Members KYC'd

KYC Date

[redacted]

Format

[redacted]

Certificate Link

[redacted]

THE TEAM

⚠️ The team is annonymous

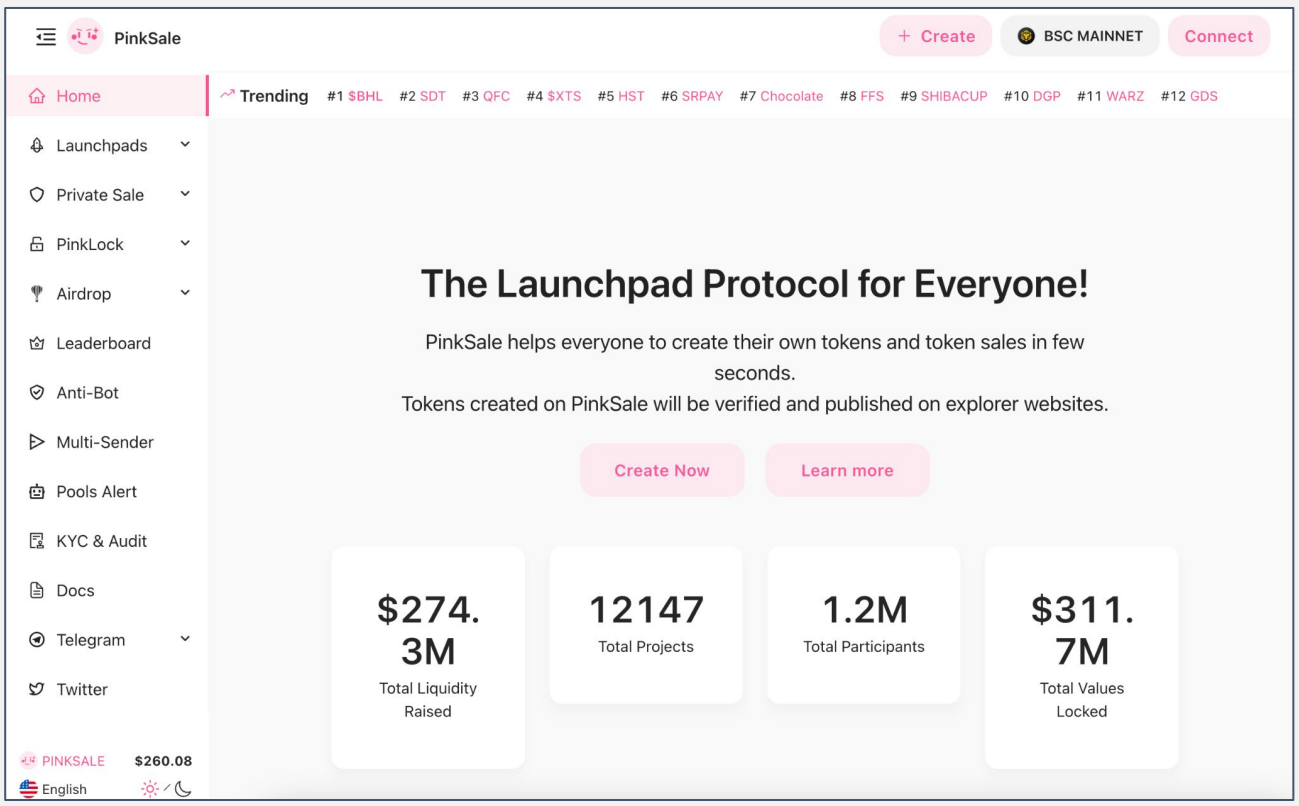
KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.

THE TEAM

The team has privately doxxed to PINKSALE



WEBSITE

Website URL
https://stellum.io/

Domain Registry
https://www.namecheap.com/

Domain Expiration
Expires on 2023-10-19

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

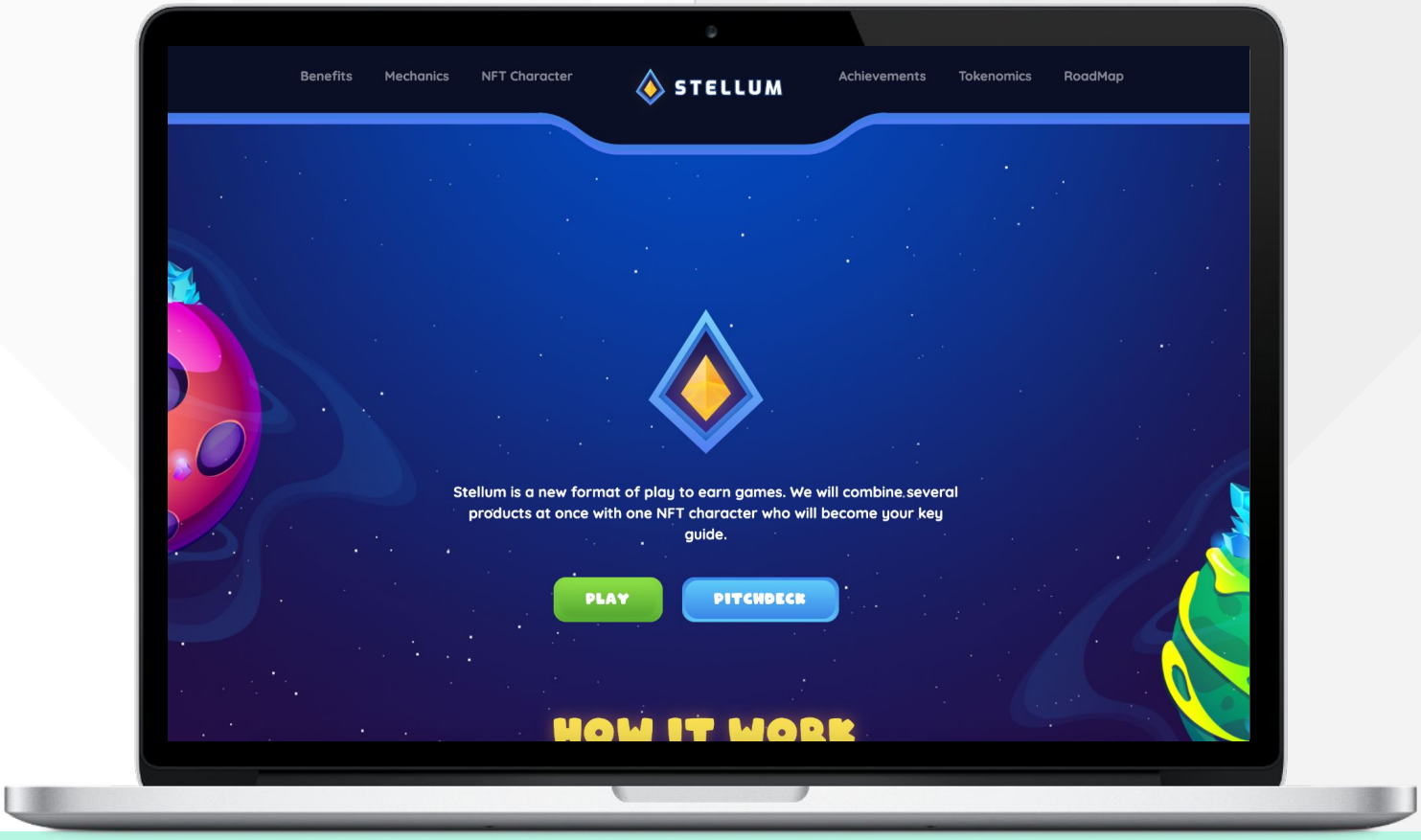
Design
Very nice unique design with appropriate color scheme and attractive graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found..

Whitepaper
Well written, explanatory.

Roadmap
Yes

Mobile-friendly?
No



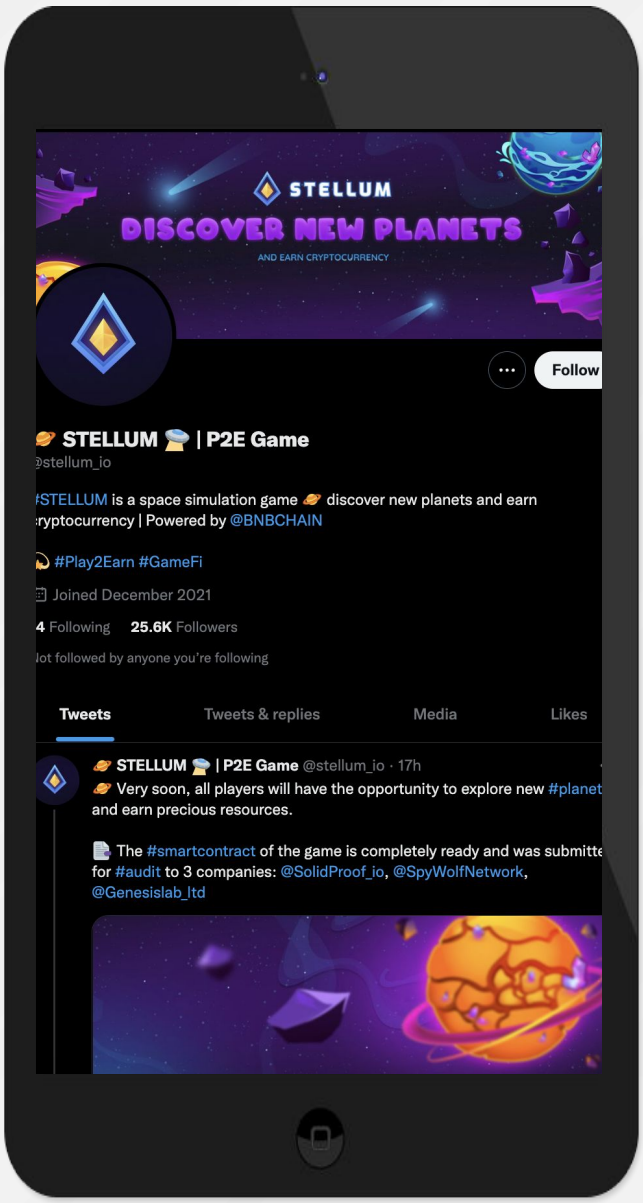
stellum.io

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Some of the project's communication channels are heavily botted



Twitter

@stellum_io

- 25 600 followers
- Active
- Posts frequently

Discord

https://discord.com/invite/fAsxGEWfu4

- 22 members
- Few active members

Telegram

@TelegramUSERNAME

- 9 104 members, botted ⚠️
- No active mods ⚠️
- No active devs ⚠️

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.